Analysis of Human-related Accidents and Assessment of Human Error Based on STAMP

Case study on a Minuteman (MM) III missile accident

Rong Hao, Tian Jin
School of Reliability and Systems Engineering
Beihang University
Overview

- Introduction
- Accident process
- STAMP-based analysis
- Human error assessment
- Conclusion
STAMP and STPA were used to analyze a MM III missile accident.

The accident causation was identified and analyzed, and the dynamics and migration of system was discussed.

Based on the accident causation, human error contributing factors was further elaborated, and the human error was quantified over time to measure system risk.
Introduction

Accident process

STAMP-based analysis

Accident causation

Human error contributing factors

System dynamics analysis

Human error assessment

SD model

Conclusions
Overview

- Introduction
- Accident process
- STAMP-based analysis
- Human error assessment
- Conclusion
MM III missile

- Conceived in the late 1950s and deployed in the early 1960s
- The only land-based Intercontinental Ballistic Missile (ICBM) in service in the United States
- In state of alert when the accident occurred on May 28, 2008.

Human involved in operation (monitoring) process of MM III

- Missile Combat Crew (MCC) 【on duty at Launch Control Center (LCC)】
  - Monitor Launch Facility (LF) and missile through Monitoring System and periodic inspections.

- Missile Maintenance Operations Center (MMOC)
  - Direct the MCC to clear the fault remotely
  - Require MCC to keep monitoring the fault in a specified time period.
  - Or send a maintenance team to the LF
Accident introduction

- On May 23, 2008, a fire broke out in Minuteman (MM) III Launch Facility (LF) A06, located near F.E. Warren AFB, WY. Fortunately, the fire did not influence missile, but the most probable total damage estimate is $1,029,855.77

- A loose connection on capacitor C101A of the battery charger inside A06’s launcher equipment room (According to Accident Investigation Board Report)
90 MMXS personnel initiated a work order to replace A06's battery charger. The modification was completed by 582 MMXS in accordance with T.O. 21 M-LGM-30 G-863, which provided inadequate direction to technicians. The LF's battery charger had a loose electrical connection on a capacitor terminal.

The new ECS was installed draws air from within the LER through its air handler. The ECS' chiller then cooled that air and recycled it back into the LER. The new ECS eliminated the addition of fresh air, called make-up air, into the LER.

An electro-mechanical maintenance team (EMT) from the 90 MMXS installed the new battery charger at A06. Between that date and 23 May 2008, the loose connection caused the charger to overcharge the batteries, which created excessive hydrogen gas ($H_2$) inside the LER.

A general site hardware and equipment configuration inspection of A06, including the LER, found no abnormalities.

The Alpha flight MCC completed crew changeover.

There were approximately eight lightning strikes within one mile of A06 between 1600 and 1700 MST.

The LF automatically switched to backup power provided by a set of batteries located in LER. A06 reported GMRs 26, 27, 28, and 29. It is normal for GMRs 26-29 to report when there is an interruption in commercial power, and they usually clear when commercial power comes back on line.

A spark or fire from the loose connection inside the battery charger ignited the gas.

A06 reported a missile suspension system fault (GMR 30). The MCC notified the MMOC of the GMRs reporting at A06.

All GMRs cleared except for a launch tube (LT) temperature alarm (GMR 28) and a missile suspension system alarm (GMR 30).

An electro-mechanical maintenance team (EMT) from the 90 MMXS went to A06 to attempt to clear the GMR 30. When they entered the LER, they discovered evidence a fire had occurred.
Overview

- Introduction
- Accident process
  - STAMP-based analysis
  - Human error assessment
- Conclusion
STEP 1: Identify the system safety constraints and system requirements

STEP 2: Document the safety control structure controlling the hazard and enforcing the safety constraints

STEP 3: Analyze the hazards at the operation process level based on STPA

STEP 4: Moving up the levels of the safety control structure, determine how and why each successive higher level allow or contribute to the inadequate control at the current level
STEP1: Identify the system safety constraints and system requirements.

- Fire accident.
- Safety constraints:
  - 1) Avoiding the *concurrence* of flammable substances, oxidizer and ignition source.
  - 2) Avoiding the *interaction* of flammable substances, oxidizer and ignition source.

STEP2: Document the safety control structure to control the hazard and enforce the safety constraints.
STAMP-based analysis

Control Structure

High level

Operation process

Management Department of Intercontinental Ballistic Missile

- Certification Standards Regulations
- Change reports
- Maintenance reports
- Operations reports
- Accident and incident reports

Improved Maintenance Management Department

- Safety standards
- Technical order
- Hazard analyses
- Progress reports

582d Missile Maintenance Squadron

- Revised
- Operating procedures
- Hardware replacements
- Software revisions

90 Missile Wing

- Safety policy
- Standards
- Resources
- Instructions

Mission Combat Crew

- Alarm reports
- Site supervision
- Power
- Temperature
- Heat or cool
- Wind

Power-Supply System

- Maintenance reports
- Direct remotely
- Ground maintenance response reports

Environmental Control System

- Maintenance team
- Launcher Facility
- Supply

Missile Maintenance Operations Center

- Maintenance team
- MM III

Operation Process

Launch Facility Monitoring System

- Parameter monitoring
- Problem reports
- Change requests
- Performance audits
- Incidents
STEP 3: Analyze the hazards at the operation process level based on STPA.
# STAMP-based analysis

## Unsafe control actions for all controllers in operation process

<table>
<thead>
<tr>
<th>Controller</th>
<th>Control action</th>
<th>a. Not Providing</th>
<th>b. Providing</th>
<th>c. Wrong Time or Order</th>
<th>d. Stopped Too Soon or Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCC</td>
<td>Report indications and actions taken to MMOC</td>
<td>No reports</td>
<td>Inappropriate or missing reports</td>
<td>Delayed report</td>
<td></td>
</tr>
<tr>
<td>Monitor LF and missile</td>
<td>Missing Monitor</td>
<td>Ignore the monitoring information and GMRs.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MMOC</td>
<td>Direct the MCC to clear the fault remotely</td>
<td>No response in the time</td>
<td>Inappropriate or wrong direction</td>
<td>Delayed direct</td>
<td></td>
</tr>
<tr>
<td>Send maintenance team to the LF</td>
<td>No response in the time</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delayed send</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch Facility Monitoring System</td>
<td>Monitor physical system operation</td>
<td>No alarm when failures occur</td>
<td>False alarm</td>
<td>Delayed alarm</td>
<td></td>
</tr>
<tr>
<td>Power-Supply System</td>
<td>Power supply</td>
<td>No automatically switched to backup power when emergency situations occur</td>
<td>Unstable electrical frequency; Leakage of electricity</td>
<td>Unexpected power outages</td>
<td></td>
</tr>
<tr>
<td>Environmental Control System</td>
<td>Control the temperature and humidity in LF</td>
<td>Invalid temperature and humidity control; Inappropriate parameter test</td>
<td></td>
<td>Too high or too low control sensitivity</td>
<td></td>
</tr>
</tbody>
</table>
Process model for operation process.

- **Ground maintenance response reports**
  - Maintenance reports
  - Direct remotely

- **Power-Supply System**
  - *Process model*
    - Normal power supply function
    - **Backup function**
      - Power switch

- **Missile Combat Crew**
  - *Process model*
    - Report indications and actions taken to MMOC GMRs
    - Monitor LF and missile equipments in LF

- **Environmental Control System**
  - *Process model*
    - Parameter test
    - Temperature
    - Humidity
    - **Function output**
      - Heat or cool air
      - Wind

- **Launcher Supply Facility**
  - *Process model*
    - Fixed supporting for missile
    - Environment supply
    - Power supply

- **Launch Facility Monitoring System**
  - *Process model*
    - Equipment monitoring
    - LF missile
    - **Function output**
      - Alarm Report

- **Alarm reports**
  - Site supervise

- **Maintenance team**

- **MM III**

- **Maintenance team sending**
  - Direct the MCC remotely T.O
  - maintenance team sending

- **Parameter monitoring**
Causal factor analysis

- **Missile Combat Crew**
  - Missing or wrong implementation of orders and instructions from 90MW
  - Delayed response to emergency situations
  - **Process model incorrect**
    - Thought LF and missile in good condition when it is not
    - Thought the GMRs are false alarm when it is not

- **Power-Supply System**
  - Missing stabilize voltage
  - Leakage of electricity
  - **Process model incorrect**
    - Missing power switch when in emergency
    - Unexpected power outages

- **Environmental Control System**
  - Safety requirements of control of temperature and humidity not implemented correctly
  - **Process model incorrect**
    - Function output not implemented correctly according to settings

- **Environmental Control System**
  - Heat or cool
  - Wind Control
  - Wrong or Delay
  - Inaccurate Temperature

- **Launch Facility Monitoring System**
  - Alarm function failure
  - **Process model incorrect**
    - No alarm when failures occur
    - False alarm in normal condition

- **Missile Maintenance Operations Center**
  - Missing or wrong implementation of orders and instructions from 90MW
  - Requirement from MCC not implemented correctly
  - **Process model incorrect**
    - Thought LF and missile in good condition when it is not
    - Thought the GMRs are false alarm when it is not

- **Launcher Facility**
  - Flammable substances occur in LF
  - **Process model incorrect**
    - No alarm when supply to missile not implemented

- **MM III**
  - Supply cut-off

- **Ground Maintenance Response**
  - Reports Error or Delay

- **Delay Maintenance Reports**
  - Error Direct remotely

- **False Alarm Reports**
  - Delay or Miss
  - Site Supervising

- **Maintenance Team Delay**
  - Delay Maintenance Reports

- **Maintenance Team Delay**
  - Maintenance Response

- **Inaccurate or Delay parameter monitoring**

- **Flammable substances**
The structure at the time of the accident

- **Missile Combat Crew**
  - Missing or wrong implementation of orders and instructions from 90MW
  - **Process model incorrect**
    - Thought LF and missile in good condition when it is not
    - Thought the GMRs are false alarm when it is not

- **Power-Supply System**
  - the loose connection of battery charger created excessive hydrogen gas
  - the loose connection of battery charger caused a spark or fire

- **Environmental Control System**
  - **dysfunctional interactions**
    - eliminated the addition of fresh air, called make-up air, into the LER

- **Launch Facility Monitoring System**
  - Launch Reports
  - Delay or Miss Site Supervising

- **Missile Maintenance Operations Center**
  - **Process model incorrect**
    - Thought the GMRs are false alarm when it is not

- **Launcher Supply Facility**
  - Flammable substances occur in LF

- **MM III**
  - Supply

**half of structure is ineffective**
Loose connection on capacitor of the battery charger caused the emergence of flammable substances (H\textsubscript{2}) and ignition source (electrical arcing caused a fire or spark)

MCC, MMOC and other controllers were neither in the right place, nor inspected periodically when accident happened, which triggered the interaction of flammable substances, oxidizer and ignition source.

Inadequate human-related control in operation process is exacerbated with the degraded quality of physical system (e.g. the false alarm).

Dysfunctional interaction:
New ECS eliminated the addition of fresh air into the LER, exacerbated the accumulation of H\textsubscript{2}. 

STAMP-based analysis
STEP4: Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level.
Analysis of controllers in high level

90 Missile Wing
Safety Requirements and Constraints:
• Propose specific plans of training and task according to orders from 90MW
• Control and management of MCC and MMOC in operation process, keep communication and coordination between them
• Supervision of MCC and MMOC to ensure safe operation process

The controller operation:
• Orders, Standards and Regulations from Management Department of Intercontinental Ballistic Missile missing or wrong, such as flammable substance management rule
• Incomplete safety culture construction
• Thought MCC and MMOC receive order or task plan information when it is not
• Thought MCC and MMOC implement task plan correctly when it is not

Actuators and controlled processes:
• Task plan conveying flaw

Context and environment in which the human is working:
• Pressure of resources or finance on supervision and management of MCC and MMOC
• Implement management according to the old experience
• Lack of communication to MCC and MMOC

582d Missile Maintenance Squadron
Safety Requirements and Constraints:
• Implement equipment improved maintenance plan according to orders from Improved Maintenance Management Department
• Provide logistics support for operation process
• Responsible for maintenance, repair, overhaul, and modification in operation process
• Report problems and maintenance related information to Improved Maintenance Management Department

The controller operation:
• Equipment improved maintenance plan and technical documentation from Improved Maintenance Management Department missing or wrong
• Inappropriate technical documentation including T.O.
• Thought LF and missile in good condition when it is not
• Delayed update equipment improved maintenance plan and technical documentation
• Problem report and safety report missing

Actuators and controlled processes:
• Maintenance error caused equipment failure

Context and environment in which the human is working:
• Insufficient training for solider

Coordination and Communication among controllers and Decision makers:
• Resources pressure and financial pressure on human error
Analysis of controllers in high level

Management Department of Intercontinental Ballistic Missile

Safety Requirements and Constraints:
- Keep communication and coordination between operation and maintenance management department.
- Develop safety related certification, standards and regulations
- Supervision and control of 90MW and Improved Maintenance Management Department to ensure operation and maintenance safety
- Safety decisions based on reports from 90MW and Improved Maintenance Management Department
- Propose plans of equipment development and improvement, ensure safety requirements satisfied and assurance the quality.
- Provide safety information feedback channels for 90MW and Improved Maintenance Management Department

The controller operation:
- Thought safety management and techniques implemented effectively in operation process when it is not
- Thought safety measures effective when it is not
- Thought risk level is low when there is no accident happened in operation process
- Delayed or missing accident report and hazard report from low level controllers

Actuators and controlled processes:
- Insufficient safety requirement conveyed to Improved Maintenance Management Department
- Insufficient or missing safety assessment of equipment improved maintenance task
- Insufficient supervision and control of 90MW and Improved Maintenance Management Department

Context and environment in which the human is working:
- Pressure from national strategies and commitment to fighting capability

Improved Maintenance Management Department

Safety Requirements and Constraints:
- Propose specific plans of equipment improved maintenance
- Develop the safety design principles in the equipment improved maintenance plan
- Supervision and management of operation in equipment improved maintenance, ensure safety requirements satisfied and assurance the quality.
- Updating of technical documentation including Technical Order(T.O.) according to the reports from operation process.

The controller operation:
- Deficiency of equipment improved maintenance Quality Assurance procedure
- Thought the improved equipments satisfied the safety requirements in operation process
- Thought safety measures effective when it is not

Actuators and controlled processes:
- Delayed or wrong update design and safety technical documentation

Context and environment in which the human is working:
- Pressure of equipment improving schedule from Safety Management Department of Intercontinental Ballistic Missile
- Insufficient training for soldiers
Management department thought that the missile itself is more important than other supporting equipments in LF, and techniques more significant than management, which risked a huge misallocation of resources. Thus the improving plan of supporting equipments was ignored (unlike MM III), technical documents was updated with delay, and discussion work of new ECS was insufficient.

Ignorance of safety management broke the human-related control in operation process, due to laxer implementations of periodical inspections, which is exacerbated with the degraded quality of physical system (e.g. the false alarm)

Missing or delayed reports from lower levels to higher levels, because management department thought safety management and techniques implemented effectively and safety measures effective in operation process when they are not
Overview

- Introduction
- Accident process
- STAMP-based analysis
- Human error assessment
- Conclusion
Most of major accidents result from a migration of the system toward decreasing safety margins over time.

Changing (human-related) factors cause the variation of system state:

- **Operation process:**
  - the quality degradation of equipments (e.g. the false alarm)
  - personal safety awareness (task pressure, personal commitment, training experience)

- **The management controllers:**
  - a contradiction between management commitment to system goal (e.g. fighting capability, profit) and that to safety
  - lax supervision and control due to a long term non-accident state and a bounce after an accident.
Measurement for system risk

- Widely used:
  accident/incident rate

- Human-related accident:
  Human Error Probability (HEP) was used

- Advantage:
  - based on Human Reliability Analysis (HRA) that has been relatively developed.
  - a more specific measurement than general accident/incident rate
Human error contributing factors:

- management
- task pressure
- experience
- safety awareness
- equipment quality degradation

All the factors change over time, so the HEP is probably a changing variable from a view of long term.

System Dynamics was used to analyze the complex relationship among these factors.
Human error assessment

The figure describing causal relation
Human error assessment

System module

- Fighting Capability Pressure Effect Time
- Fighting Capability Priority Exponent
- Human Error Effect Time on Management Commitment to Safety
- Human error Exponent on Management Commitment to Safety
- Target Management Commitment to Safety
- Change in Management Commitment to Safety
- Relative Management Commitment to Fighting Capability
- Change in Management Commitment to Fighting Capability
- Time to Change Management Commitment to Safety
- Target Management Commitment to Fighting Capability
- Pressure to Change Management Commitment to Safety
- Effect of Equipment Technology Level on Management Commitment to Fighting Capability
- Effect of Equipment Technology Level on Management Commitment to Safety
- Reference Equipment Technology Level
- Effect of Management Commitment to Safety on Management Commitment to Fighting Capability
- Human Error Effect Exponent on Management Commitment to Safety
- Relative Equipment Technology Level

Total Experience
- Loss of Experience from attrition
- Increase in Experience from hiring
- Increase in Experience from training
- Increase in Experience from Task
- Increase in Experience from Training and Task

Current Number of Soldier
- Hiring
- Quit
- Hiring Time
- Gap in Hiring Number
- Target Hiring Demand
- Total Working Hours Per Year
- Average Working Hours Per Year
- Management Commitment Effect Time on Personal
- Change in Personal Commitment to Safety
- Time to Change Personal Commitment to Safety
- Target Personal Commitment to Safety
- Time to Provide Training Referenced Experience
- Increase in Experience from Training
- Decrease in Experience from Training and Task

Relative Average Experience
- Reference Average Experience

Relative Personal Commitment to Safety
- Reference Personal Commitment to Safety
- Effect of Relative Personal Commitment on quit

Average Experience of Rookies Hired
- Total Average Experience

Human error
- Human Error Effect Time on Personal Commitment to Fighting Capability
- Primary Human Error Exponent on Personal Commitment to Fighting Capability
Results and discussion

Management Commitment to Safety

Management Commitment to Fighting Capability

Personal Commitment to Safety

HEP

high risk
Human error contributing factors should be focused on
- experience, personal commitment (safety awareness), pressure, equipment technology level (e.g. man-machine interface)

The human-related variables fluctuate in the early time period, with the amplitude getting less
- Because management has effect on personal commitment, but the effect is decreasing due to degenerate physical system.
- some measurements should be adopted to keep HEP as low as possible:
  - better equipment technology level
  - management pay enough attention on human error

HEP keeps increasing during the mid-late period
- degenerate physical system is dominant in contributing factors
- the critical increasing/decreasing factors (e.g. equipment technology level) should be focused more on
Overview

- Introduction
- Accident process
- STAMP-based analysis
- Human error assessment
- Conclusion
In operation process, prevent the failures of all controllers to missile in the same time.

(MCC, MMOC, Monitoring system)

Management department should pay balanced attention to each aspect in the system, by changing its “process model”

- safety & fighting capability, management & technology

Better control and feedback channel to ensure the real system state informed to all controllers

Analyze accident causes from a view of system

- not just replace the battery charger
Thanks!

email:  Rong Hao  ronghao2010@sina.com
       Tian Jin   rabbit-tian@163.com